



Professional Indemnity Cyber and Data Protection Law Endorsement

For the avoidance of doubt, save as expressly provided in this endorsement, or by other restrictions in this policy specifically relating to the use of, or inability to use a **computer system**, no cover otherwise provided under this policy will be restricted solely due to the use of a **computer system**.

This policy does not cover any **claim**, loss, damage, liability, costs, expenses, fines, penalties, mitigation costs or any other amount directly caused by, directly resulting from or directly arising out of:

- a) a **security event**
- b) any partial or total unavailability or failure of any **computer system**

Provided the **computer system** is owned or controlled by the **insured** or any other party acting for and behalf of the **insured**.

This policy does not cover any **claim**, loss, damage, consequential loss, liability, costs, expenses, fines, penalties, mitigation costs or any other amount directly or indirectly caused by, directly or indirectly resulting from or directly or indirectly arising out of:

- i) a **power failure** but only where such **power failure** impacts a **computer system** owned or controlled by the **insured** or any other party acting on behalf of the **insured**
- ii) any failure or interruption of service provided to the **insured** or any other party acting on behalf of the **insured** by an internet service provider, telecommunications provider or cloud provider but not including the hosting of hardware and software owned by the **insured**.

This policy does not cover any **claim**, loss, damage, consequential loss, liability, costs, expenses, fines, penalties, mitigation costs or any other amount for a breach of **data protection law** by the **insured** or any other party acting on their behalf.

Any cover provided under this policy for costs of reconstituting or recovering lost, inaccessible or damaged documents owned or controlled by the **insured** or any other party acting on behalf of the **insured** will not apply to **electronic data**.

Definitions

Computer system

Computer hardware and software and the electronic data stored thereon including associated input and output devices, data storage devices, networking equipment,



components, firmware and electronic back up facilities including systems available through the internet, intranets, extranets or virtual private networks.

Computer system also means any of the foregoing that are part of an Industrial Control System.

Data protection law

Any applicable data protection and privacy legislation or regulations in any country, province, state, territory or jurisdiction which govern the use, confidentiality, integrity, security and protection of personal data or any guidance or codes of practice relating to personal data issued by any data protection regulator or authority from time to time (all as amended, updated or re-enacted from time to time).

Electronic data

Information stored or transmitted in digital format. **Electronic data** does not include software or digital currency and or cryptographic key material providing access to digital currency systems.

Power failure

Any mechanical or electrical failure, interruption or outage including any electrical power interruption or surge, brownout, blackout, short circuit, over voltage or power fluctuation or outage to gas, water, telephone, cable, satellite, telecommunications, the internet or any component thereof including hardware or software or any other infrastructure.

Security event

a) The receipt or transmission by an **insured** or any other party acting on behalf of the **insured** of any unauthorised, corrupting or harmful software, code or program specifically designed to erase or corrupt **electronic data**, or damage or disrupt any network or **computer system** or circumvent any security product or service including but not limited to computer viruses, Trojan horses, worms and logic bombs

b) unauthorised, malicious or criminal act or series of related unauthorised, malicious or criminal acts, regardless of time or place or the threat or hoax thereof involving access to or use of a **computer system** or other equipment or component or system or item which processes, stores, transmits, retrieves or receives data

c) any actions or instructions constructed or generated with the ability to damage, interfere with or otherwise affect the availability of networks, network services, network connectivity or information systems including but not limited to the generation of excess network traffic into network addresses, the exploitation of system or network weaknesses and the generation of excess or non-genuine traffic between and amongst networks.